The memoirs and legacy of Évariste Galois

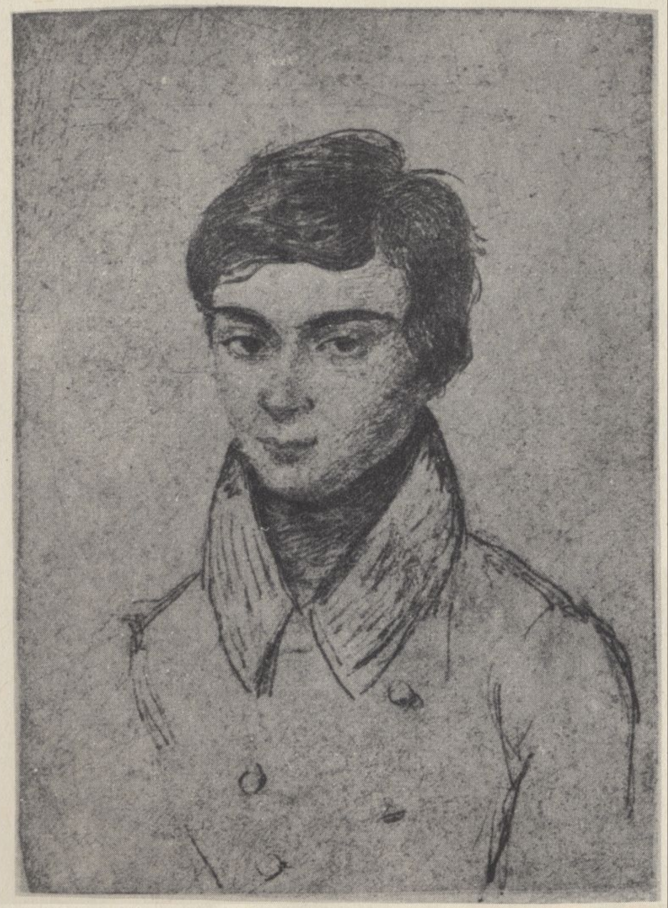
BSHM Gresham Lecture, Gresham College:

Thursday 3 November 2011

Peter M. Neumann (Queen's College, Oxford)

- Évariste Galois—a sketch of his life
- His memoirs—the main works
- Equations
- Groups
- The mathematical legacy of Évariste Galois

Portrait d'Evariste Galois, fait de mémoire par son frère Alfred en 1848.
(Magasin pittoresque. Juillet 1848, 3e semaine, tome XVI, p. 227).



Portrait d'Evariste Galois à quinze ans.
(Annales de l'Ecole Normale Supérieure - 3e série. Tome XIII, 1896)

Depictions of Galois

Évariste Galois: a brief *cv*

25 Oct 1811	Évariste Galois born (Bourg-la-Reine, near Paris)
Oct 1823	Enters Collège Louis-le-Grand; stays six years
25 May 1829	First submits mathematical discoveries to Academy
2 July 1829	Father's suicide
July 1829	Second and final rejection by École Polytechnique
Oct 1829	Enters École Préparatoire (= Éc. Norm. Sup.)
12 Feb 1830	Second submission to Academy: manuscript lost
Dec 1830	Expelled from college
17 Jan 1831	Submits <u>Premier Mémoire</u> to Academy
May 1831	Arrested for offensive behaviour; acquitted 15 June
4 July 1831	<u>Premier Mémoire</u> rejected by Academy
14 July 1831	Imprisoned for 9 months; released 29 April 1832
30 May 1832	Shot in a mysterious early-morning duel
31 May 1832	Died.

Évariste Galois, révolutionnaire et géomètre

Title of a novel by André Dalmas, 1956

The Memoirs of Évariste Galois

- Sur la théorie des nombres
  Published June 1830 in Férussac's Bulletin
- Mémoire sur les conditions de résolubilité des équations par radicaux
  known as the Premier Mémoire
  Contains 'Galois Theory' of equations
  Rejected July 1831 by Paris Academy of Science published 1846, 1889, 1897, 1951, 1962, 1984, 2011, . . .
  N.B. Two predecessors of this work are lost
- Des équations primitives qui sont solubles par radicaux
  known as the Second Mémoire
  Published 1846, etc. Probably written May/June 1830
- Lettre à Auguste Chevalier, Paris, le 29 Mai 1832
  A testamentary summary of Galois' discoveries.
  Published 1832, 1846, etc.

Also a few articles published when he was 17 or 18

The manuscripts

Held in library of the Institut de France

285 folios; various shapes and sizes; bound as 1 volume;
c. 200 in Galois' hand; the rest written by Chevalier, Liouville

Organised into 27 dossiers; most important are dossiers 1–5:
Dossier 1: Premier Mémoire
Dossier 2: Lettre testamentaire
Dossier 3: copy by Chevalier of Premier Mémoire, and more
Dossier 4: Second Mémoire
Dossier 5: copy by Chevalier of Second Mémoire

Dossiers 6–25: fragments. Some interesting mathematics; some philosophical-polemical writings; scraps with unexplained calculations and jottings.
Dossier 26: some of Galois' school exercises.
Dossier 27: some Liouville material.

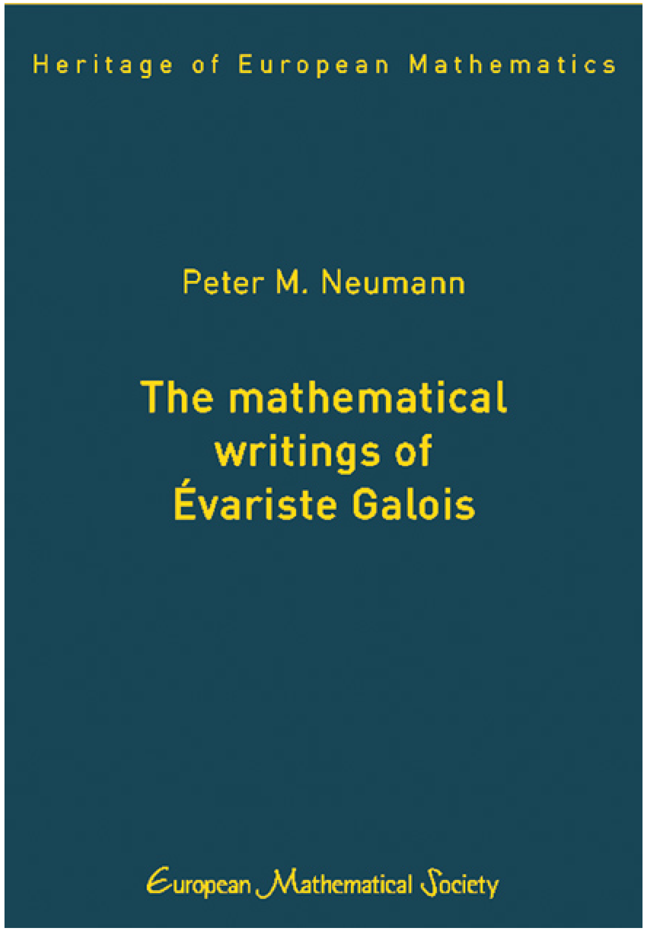
Many editions since 1846; the most recent (2011):

Peter M. Neumann

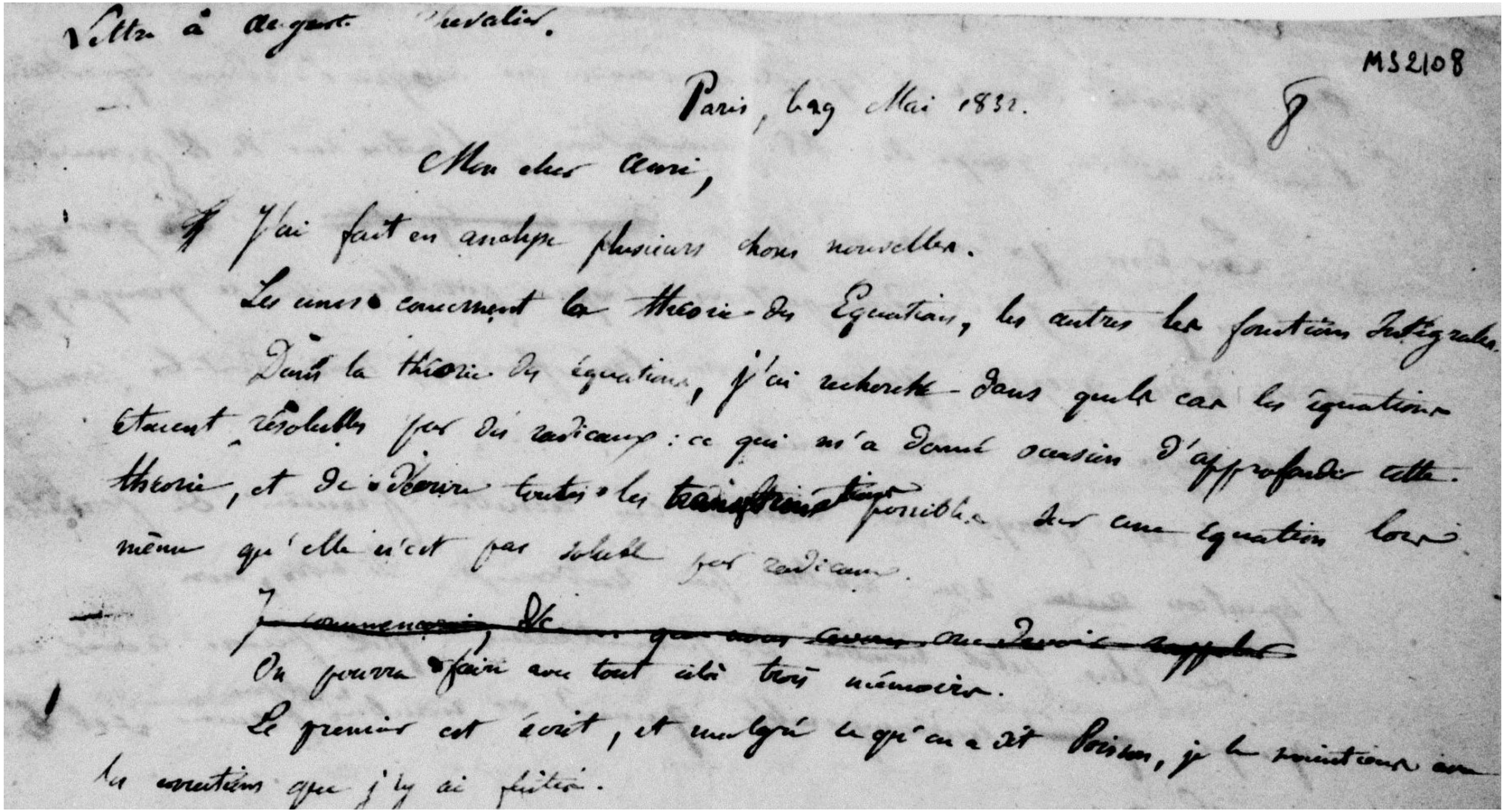
The mathematical writings
of Évariste Galois

European Mathematical Society,
25 October 2011

ISBN 978-3-03719-104-0



Galois' theory of equations and groups


Lettre à Auguste Chevalier.

MS2108

Paris, le 29 Mai 1832.

Mon cher ami,

J'ai fait en analyse plusieurs choses nouvelles.

Les unes concernent la théorie des Équations, les autres les fonctions Intégrales.

Dans la théorie des équations, j'ai recherché dans quels cas les équations étaient résolubles par des radicaux: ce qui m'a donné occasion d'approfondir cette théorie, et de décrire toutes les transformations possibles sur une équation lors même qu'elle n'est pas soluble par radicaux.

~~[illegible]~~

On pourra faire avec tout ceci trois mémoires.

Le premier est écrit, et malgré ce qu'en a dit Poisson, je le maintiens avec les corrections que j'y ai faites.

Beginning of the Testamentary Letter, 29 May 1832

Equations: degree 1

Problem: **solve the equation**

$$5x - 10 = 0$$

Equations: degree 1

Problem: **solve the equation**

$$5x - 10 = 0$$

Answer: $x = 2$

Equations: degree 2

Problem: **solve the equation**

$$5x^2 - 10x - 5 = 0$$

Equations: degree 2

Problem: **solve the equation**

$$5x^2 - 10x - 5 = 0$$

Answer: $x = 1 + \sqrt{2}$ **<u>or</u>** $x = 1 - \sqrt{2}$

The general cubic equation

If $x^3 + bx^2 + cx + d = 0$ **then**

$$x = -b + \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4}{27}p^3}\right)} + \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4}{27}p^3}\right)},$$

where

$$p := -\frac{1}{3}b^2 + c, \quad q := \frac{2}{27}b^3 - \frac{1}{3}bc + d\,.$$

For example, if $5x^3 + 10x^2 - 5x - 5 = 0$ **then** $x^3 + 2x^2 - 1x - 1 = 0$ **and in fact**

$$x = \tfrac{1}{3}\left(-2 + \sqrt[3]{\tfrac{1}{2}\left(-7 + \sqrt{-1323}\right)} + \sqrt[3]{\tfrac{1}{2}\left(-7 - \sqrt{-1323}\right)}\right)\,.$$

Higher degree equations

What about quartics?

What about quintics? sextics? . . . ?

The focus of the classical theory of equations

Consider the equation of degree n

$$ax^n + bx^{n-1} + \cdots = 0$$

where $a \neq 0$ and $n \geqslant 1$.

Find a formula in the coefficients a, b, $\ldots$ involving only the operations $+$, $-$, $\times$, $\div$, together with $\sqrt[k]{}$ for any k you wish, that describes a root of the equation.

Theorem. There is no such formula if $n \geqslant 5$

Finally proved satisfactorily by N H Abel (aged 21) in 1824, published 1826.

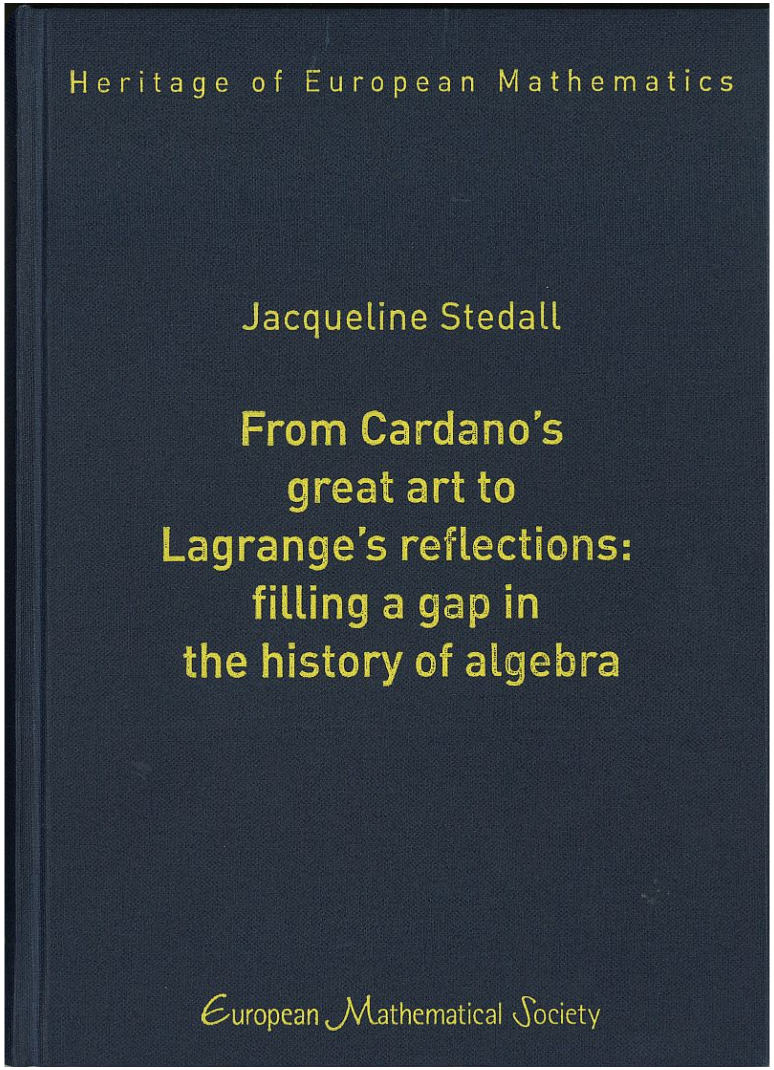
Classical algebra: a strongly recommended book

Jacqueline Stedall

From Cardano's great art
to Lagrange's reflections:
filling a gap in the history of
algebra.

European Mathematical Society,
April 2011

ISBN 978-3-03719-092-0



Equations: a subtler question

Given a particular equation with numerical coefficients is there a solution in terms of radicals?
That is, a solution in terms of numbers obtained by starting from the coefficients and using arithmetical operations and root extractions, numbers such as $\sqrt{2}$, $\sqrt[5]{(3-\sqrt{5})}$, . . .?

Sometimes YES: $x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 2 = 0$.

Sometimes NO: $x^5 + 10x^2 - 2 = 0$.

How are equations that <u>are</u> soluble by radicals distinguishable from those that are <u>not</u> ?

Galois and his groups, I

How are equations that are soluble by radicals distinguishable from those that are not?

Galois' answer: there is a group associated with every polynomial

AND: solubility by radicals can be expressed as a structural property of that group.

The group is now known as the Galois group of the polynomial; the theory as Galois Theory.

Groups: Permutations and substitutions

Cauchy 1815:

Permutation := arrangement: e.g. (3 5 2 1 4)

Substitution := change from one arrangement to another:

e.g. $\begin{pmatrix} 3 & 5 & 2 & 1 & 4 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$

Note: Galois, in 1830–32, usually used this terminology but sometimes used 'permutation' for 'substitution' (as in modern usage).

Galois and his groups, II

What the academy referees, Poisson and Lacroix, saw in 1831:

Premier Mémoire, Proposition I. Let an equation be given of which the m roots are $a, b, c, \ldots$. There will always be a group of permutations of the letters $a, b, c, \ldots$ which will enjoy the following property:

1. That every function of the roots invariant under the substitutions of this group will be rationally known;

2. Conversely, that every function of the roots that is rationally determinable will be invariant under the substitutions.

NOTE: this is <u>first</u> mention of groups in Premier Mémoire

What Poisson and Lacroix saw

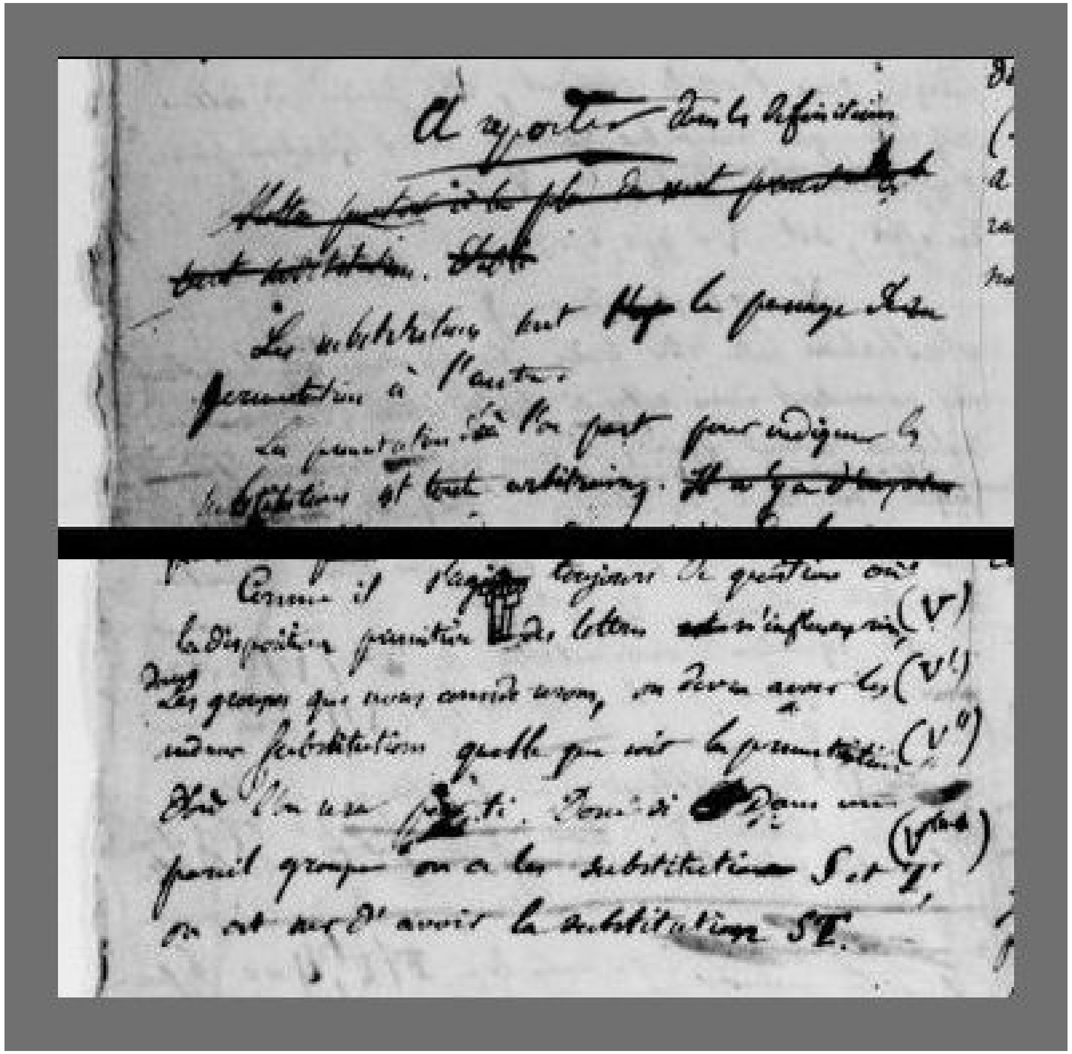
- **Proposition I and the preceding four lemmas**

- **Examples:**
  - **the 'general equation' of degree n**
  - **the equation $\dfrac{x^n - 1}{x - 1} = 0$ [for prime n]**

- **Proof of Proposition I**

- **Scholium: exiguous explanation of groups.**

The eleventh hour marginal addition to Prop I


À ajouter dans la définition

Les substitutions sont le passage d'une permutation à l'autre.

La permutation dont l'on part pour indiquer les substitutions est toute arbitraire.

[redacted]

Comme il s'agit toujours de questions où la disposition primitive des lettres n'influe en rien, dans les groupes que nous considérons, on devra avoir les mêmes substitutions quelle que soit la permutation d'où l'on sera parti. Donc si dans un pareil groupe on a les substitutions S et T, on est sûr d'avoir la substitution ST.

Galois and his groups, III

The eleventh hour marginal addition in translation:

Substitutions are the passage from one permutation to another.

The permutation from which one starts in order to indicate substitutions is completely arbitrary, . . .

. . . one must have the same substitutions, whichever permutation it is from which one starts. Therefore, if in such a group one has substitutions S and T, one is sure to have the substitution ST.

Galois and his groups, IV: summary

Groupe de substitutions: a collection of substitutions such that if S, T are any of them then also ST is in the collection

Groupe de permutations: a collection of permutations (arrangements) of the form AS, where A is a starting permutation and S ranges over a group of substitutions

BUT in the first instance the word groupe is an informal word. Galois perpetrated definition by context from which it naturally, perhaps accidentally, acquired a special meaning

AND there is a criterion for solubility of an equation by radicals in terms of structure of its group of substitutions

The mathematical legacy of Évariste Galois

Galois gave us:

- **Groups,**
- **Fields,**
- **Galois Theory and the beginnings of**
- **“modern” or “abstract” algebra**

Myths and mysteries

(1) Myth: Galois invented group theory on the night before the duel in 1832. Nonsense!

(2) Myth: Galois knew and used the simplicity of alternating groups. Nonsense

(3) Mystery: why was it that for two years before his death Galois failed to write down his ideas, as he had done from May 1829 to June 1830?

(4) Mystery: How was it that, in 1843, over ten years after the fatal duel, and when Galois was all but forgotten, Liouville recognised the basic truth and value of Galois' ideas?

Évariste Galois, géomètre révolutionnaire

We owe "MODERN ALGEBRA" to this wayward young genius, dead at the age of twenty.